DETAILED ACTION

Claims 1 – 2, 5 – 8, and 11 - 15 are allowed over the prior art of record.

Claim 16 is cancelled.

EXAMINER'S AMENDMENT

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Philip McKay, Reg. No. 38, 966, on September 17, 2009.

In the Claims:

Please amend claims 1, 7, and 13 as follows:

1. An anti-malware file scanning system for computer files being transferred between computers, the system being implemented on a computer apparatus and comprising:

a) a computer database containing records of known executable programs which are deemed to be not malware and criteria by which a file being processed can be determined to be an instance of one of those programs, the criteria including at least one characteristic signature associated with each said instance;

b) means for processing a file being transferred between computers, the means b) comprising:

a file recogniser operative to determine whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances; ~~and~~

a difference checker operative, in the case that the file recogniser determines the file being processed to be an instance of a known program, to check whether the file is an unchanged version of that known program; ~~and~~

c) means for signalling the file, depending on the determination made by the processing means, as being:

likely to be not malware if it is an unchanged version of a known file;

likely to be malware if it is a changed version of a known file; or

of unknown status if it is not determined as being an instance of a known file;

wherein the processor assigns a score to a file identified as likely to be malware, and

storing the determination that the file is likely to be not malware, is likely to be malware or is of unknown status.

7. A method of anti-malware scanning computer files being transferred between computers, the method comprising:

maintaining a computer database containing records of known executable programs which are deemed to be uninfected and criteria by which a file being processed can be determined to be an instance of one of those programs, the criteria including at least one characteristic signature associated with each said instance;

processing a file being transferred between computers by determining whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said at least one characteristic signature associated with the said instances, and

checking, in the case that the file is determined to be an instance of a known program, whether the file is an unchanged version of that known program;

signalling the file, depending on the determination made by the processing, as being:

likely to be not malware if it is an unchanged version of a known file;

likely to be malware if it is a changed version of a known file; or

of unknown status if it is not determined as being an instance of a known file;

wherein the processor assigns a score to a file identified as likely to be malware, and

storing the determination that the file is likely to be not malware, is likely to be malware or is of unknown status.

13. An anti-malware file scanning system for computer files being transferred between computers, the system comprising:

a computer database containing records of known executable programs which are deemed to be not malware and criteria by which a file being processed can be determined to be an instance of one of those programs, the criteria including at least one characteristic signature associated with each said instance;

a processor for processing a file being transferred between computers,

the processor being operative to determine whether the file being processed is an instance of a known program by checking the contents of the file being processed for the presence of said att least one characteristic signature associated with the said instances and, in the case that the file being processed is determined to be an instance of a known program,

to check whether the file is an unchanged version of that known program,

said processor, depending on the determination, identifying the file being processed as:

(i) likely to be not malware if it is an unchanged version of a known file;

(ii) likely to be malware if it is a changed version of a known file; or

(iii) of unknown status if it is not determined as being an instance of a known file;

wherein the processor assigns a score to a file identified as likely to be malware, and

storing the determination that the file is likely to be not malware, is likely to be malware or is of unknown status.

Please cancel claim 16.

Reasons For Allowance

Claims 1 – 2, 5 – 8, and 11 - 15 are allowed over the prior art of record.

Claim 16 is cancelled.

The following is an examiner's statement of reasons for allowance:

The prior art of record does not teach or fairly suggest the system or method as recited in independent claims 1, 7, or 13.

The method and system of the independent claims require the steps of determining if a file being processed is an instance of a known program by checking the contents of the file for at least one characteristic signature associated with the said instance, checking if the file is a changed or unchanged version of a known program, signaling the file if it is likely, unlikely, or unknown that malware exists within the file, assigning a score to a file, and storing the determination of the status of the file.

The dependent claims, being definite, further limiting, and fully enabled by the specification are also allowed.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ALEXANDRIA Y. BROMELL whose telephone number is (571)270-3034. The examiner can normally be reached on M - R 9 - 3.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John R. Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Alexandria Y Bromell/
Examiner, Art Unit 2167
September 19, 2009

/Shahid Al Alam/
Primary Examiner, Art Unit 2162

/John R. Cottingham/

Supervisory Patent Examiner, Art Unit 2167